AO 91 (Rev. 11/82)

CRIMINAL COMPLAINT

UNITED STATES DISTRICT COURT	CENTRAL DISTRICT OF CALIFORNIA
UNITED STATES OF AMERICA v. KIERRA PEARL AMOS, Defendant.	DOCKET NO. MAGISTRATE'S CASE NO. 17- 17-1390M

Complaint for violation of Title 18, United States Code, Sections 1029(a)(2)

NAME OF MAGISTRATE JUDGE		LOCATION
HONORABLE	UNITED STATES MAGISTRATE JUDGE	Los Angeles, California

DATE OF OFFENSE	PLACE OF OFFENSE	ADDRESS OF ACCUSED (IF KNOWN)
May 24, 2017	Los Angeles County	

COMPLAINANT'S STATEMENT OF FACTS CONSTITUTING THE OFFENSE OR VIOLATION:

[18 U.S.C. § 1029(a)(2): Use of Unauthorized Access Devices]

On or about May 24, 2017, in Los Angeles County, within the Central District of California, defendant KIERRA PEARL AMOS knowingly and with intent to defraud trafficked in or used one or more unauthorized access devices, and by such conduct obtained items valuing more than $1000.

BASIS OF COMPLAINANT'S CHARGE AGAINST THE ACCUSED:

(See attached affidavit which is incorporated as part of this Complaint)

MATERIAL WITNESSES IN RELATION TO THIS CHARGE: N/A

Being duly sworn, I declare that the foregoing is true and correct to the best of my knowledge.	SIGNATURE OF COMPLAINANT Robert Hawkeye Norman /s/ OFFICIAL TITLE Special Agent – United States Secret Service

Sworn to before me and subscribed in my presence,

SIGNATURE OF MAGISTRATE JUDGE[1]	DATE
JACQUELINE CHOOLJIAN	6/2/17

[1] See Federal Rules of Criminal Procedure 3 and 54

AUSA A. Carley Palmer x0282

AFFIDAVIT

I, Robert Hawkeye Norman, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint against and arrest warrant for KIERRA PEARL AMOS ("AMOS") for a violation of Title 18, United States Code, Section 1029(a)(2) (use of unauthorized access devices).

2. This affidavit is also made in support of an application for a warrant to search 1378 West Jenner Street, Lancaster, California 93534 (the "AMOS HOME"), as more fully described in Attachment A. The application seeks authorization to seize evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1028A (aggravated identity theft), 1029 (access device fraud), 1341 (mail fraud), and 1344 (bank fraud), as more fully described in Attachment B. Both Attachments A and B are incorporated by reference herein.

3. The facts set forth in this affidavit are based on my personal observations, my training and experience, my conversations with fellow law enforcement officers, and my involvement in this investigation, including my review of surveillance videos and reports, delivery records, and bank records. This affidavit is intended to show merely that there is sufficient probable cause for the requested arrest and search warrants, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically

indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGROUND FOR SPECIAL AGENT ROBERT HAWKEYE NORMAN

4. I am a Criminal Investigator with the United States Secret Service ("USSS") and have been so employed since May 2016. I am currently assigned to the USSS Los Angeles Field Office Financial Crimes Investigations Squad, which investigates bank fraud, access device fraud, identity theft, and the unauthorized use of others' information for financial gain.

5. As a Criminal Investigator, I participate in investigations regarding identity theft, access device fraud, and bank fraud. I have completed the 12-week Criminal Investigator Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia. That course included training in the investigation of identity theft, mail fraud, internet crimes, and access device crimes. I have also completed the 18-week USSS Special Agent Training Program at the James J. Rowley Training Center in Laurel, Maryland. That course included training for investigations regarding mail fraud, wire fraud, and access device fraud.

6. Before joining the USSS, I served 15 years in the United States Marine Corps, earning the rank of Gunnery Sergeant. During my last 10 years in the Marines, I was a Counterintelligence Agent and Human Resource Intelligence ("HUMINT") collector. In that role, I conducted numerous surveillance and countersurveillance operations; interviews and

interrogations; and investigations into terrorist activities, espionage, and insider threats.

7. I have a Bachelor of Arts in Psychology from the University of South Florida and a Master of Science of Strategic Intelligence from the National Intelligence University. I also have certification with highest honors in Advanced Analytical Techniques for countering adversarial denial and deception.

III. BACKGROUND REGARDING ACCOUNT TAKEOVER SCHEMES

8. Based on my knowledge, training, and experience, as well as information related to me by other law enforcement officers and USSS special agents who specialize in fraud investigations, I know the following:

a. People who execute account takeover schemes obtain access to a victim's account using personally identifiable information ("PII"), such as names, social security numbers, dates of birth, account numbers, addresses, phone numbers, and passwords. Fraudsters often obtain PII through social engineering, malicious software or Malware, email hoaxes, personal knowledge of the victim, theft, or exploitation of information safeguarding vulnerabilities. Equipped with enough PII, fraudsters can answer the identity verification questions used to allow account holders online access to their bank accounts. Once inside a system, fraudsters can view the account, change the account information, and make requests under the guise of the account holder.

b. Bank account takeovers occur when a fraudster changes such account identifiers as the Personal Identification Number ("PIN") or login information, including associated emails and passwords. The fraudster typically changes the account holders' mailing address and requests new or replacement credit and/or debit cards in the account holders' name to an address to which the fraudster has access. Fraudsters often use digital devices to make changes online, call the bank, or to send or receive account verification test messages.

c. It is common in such account takeover schemes to target victims who are typically not internet savvy or technologically inclined, such as elderly account holders. People of an older demographic are less likely to access their accounts online, set up email or text updates about account activity, or frequently monitor their accounts through smartphone applications or online access. As a result, a fraudster's online account activity may go unnoticed by the account holder for a long time, giving the fraudsters opportunity to exploit their fraudulently obtained access.

d. Once fraudsters obtain the debit or credit accords associated with compromised accounts, they use the cards as if they are their own. Transactions where the fraudsters need not interact with a teller or cashier eliminate the chance for someone to ask for an identification to match the credit or

debit card. ATM cash withdrawals require only the card and PIN, and they yield cash in the amount up to the card's daily limit.

IV. SUMMARY OF PROBABLE CAUSE

9. Between May and June 2017, a fraudster accessed several Navy Federal Credit Union ("NFCU") online bank accounts, changed the account holders' addresses of record to the AMOS HOME or another nearby address, and asked that new debit cards be delivered to the new addresses. The compromised accounts were then "cashed out" at Automatic Teller Machines ("ATMs") at 7-11 stores in Palmdale and Lancaster. Most of the withdrawals took place at a 7-11 on Sierra Highway in Lancaster (the "Sierra Highway 7-11").

10. On May 17, 2017, Federal Express ("FedEx") delivered three debit cards in the name of NFCU account holder J.A.R. to the AMOS HOME. Within an hour, the cards were activated online and money was withdrawn using successive withdrawals from the Sierra Highway 7-11 ATM. Law enforcement watched the AMOS home and saw that a gray 2004 Ford Taurus with California license plate 5PIN793 (the "AMOS CAR")[1] was at the AMOS HOME during the FedEx delivery, and left approximately 30 minutes later. AMOS went to the 7-11 in the AMOS CAR, walked into the store just before the withdrawals, and walked out of the store just after.

11. On May 18, 2017, account holder D.B.S's NFCU account was compromised, and two debit cards were ordered to the AMOS

[1] From my review of law enforcement databases, I know that the AMOS CAR is registered to AMOS at the AMOS HOME.

HOME. On May 19, 2017, law enforcement saw FedEx deliver the cards to a woman matching AMOS's description at the AMOS HOME.

12. On May 23, 2017, account holder J.M.'s account was compromised, and three debit cards were ordered to the AMOS HOME. On May 24, 2017, FedEx delivered the cards to the AMOS HOME. 24 minutes later, the cards were activated online. Eight minutes after that, AMOS used two of the cards to make successive cash withdrawals at the ATM located at the 7-11 on East Avenue I in Lancaster (the "Avenue I 7-11"). NFCU closed the account, AMOS tried unsuccessfully to withdraw money using the third card, and AMOS used the ATM to make balance inquiries regarding J.M.'s account.

13. On May 24, 2017, during a trash pull of trash cans in front of the AMOS HOME, agents found: (1) two FedEx envelopes containing the NFCU mail delivered to D.B.S. at the AMOS HOME on May 19, 2017; (2) opened mail addressed to an earlier NFCU account victim, V.K.H., at the AMOS HOME; and (3) a Southern California Edison electricity bill addressed to AMOS at the AMOS HOME.

V. STATEMENT OF PROBABLE CAUSE

A. AMOS Defrauds NFCU Using the J.A.R. Account on May 16 and 17, 2017.

14. Based on my review of NFCU bank investigative reports, my review of physical evidence, my review of 7-11 surveillance footage, my conversations with fellow law enforcement officers,

and my own observations and knowledge of the investigation, I know the following:

a. According to NFCU bank investigators and computer transactional information, on May 16, 2017, someone other than the account holder accessed the online NFCU accounts of J.A.R. of Peoria, Arizona, changed her home address to the AMOS HOME, and ordered debit cards for J.A.R.'s three accounts to be delivered by FedEx to the AMOS HOME on May 17, 2017.

b. During physical surveillance of the AMOS HOME at approximately 3:38 p.m. on May 17, 2017, I saw FedEx deliver three FedEx envelopes containing three NFCU debit cards in the name of J.A.R.

c. According to NFCU bank investigators, by 4:38 p.m., all three cards had been activated online and someone had withdrawn the $600 daily cash limit on all three credit cards, for a total of $1800, at the Sierra Highway 7-11 ATM.

d. At approximately 4:14 p.m., I saw AMOS, who I recognized from her California Department of Motor Vehicles photo, and a female companion leave the AMOS HOME in the AMOS CAR and drive northeast, toward the Sierra Highway 7-11.

e. 7-11 video surveillance at the time of the ATM cash withdrawals, that is from 4:35 p.m. to 4:42 p.m., shows the AMOS CAR arrive at the 7-11, AMOS enter the 7-11, AMOS walk out

of the 7-11 approximately seven minutes later, and the AMOS CAR leave.

f. According to California DMV records and personal observation, AMOS is a larger black woman in her early 40s with curly hair, a nose stud, and back tattoos.

B. AMOS Defrauds NFCU Using the D.B.S. Account on May 18 and 19, 2017.

g. According to NFCU bank investigators and computer transactional information, on May 18, 2017, someone other than the account holder accessed the online NFCU accounts of D.B.S. of Yuma, Arizona, changed her home address to AMOS HOME, and ordered debit cards for two accounts to be delivered by FedEx to the AMOS HOME on May 19, 2017.

h. During physical surveillance of the AMOS HOME at approximately 4:30 p.m. on May 19, 2017, USSS criminal investigators saw FedEx deliver two envelopes containing two NFCU debit cards in the name of D.B.S. The FedEx driver described the person who signed for the packages as a heavyset black woman with a nose stud.

i. During examination of trash removed from the AMOS HOME on the morning of May 24, 2017, USSS Special Agent Kyle Weeks and I found two FedEx envelopes containing NFCU mail addressed to D.B.S. at the AMOS HOME. Tracking numbers on the envelopes matched the D.B.S. card delivery tracking numbers

provided by NFCU investigators. Agents also found opened mail addressed to NFCU account holder V.K.H. at the AMOS HOME,[2] and a Southern California Edison electricity bill from addressed to AMOS at the AMOS HOME.

C. AMOS Defrauds NFCU Using the J.M. Account on May 23 and 24, 2017

j. According to NFCU bank investigators and computer transactional information, on May 23, 2017, someone other than the account holder accessed the online NFCU accounts of J.M. of Corona, California, changed her home address to AMOS HOME, and ordered debit cards for three accounts to be delivered by FedEx to AMOS HOME on May 24, 2017.

k. According to the FedEx dispatcher, at approximately 2:18 p.m. on May 24, 2017, FedEx delivered three envelopes to the AMOS home, where someone signed for them in J.M.'s name. The tracking numbers on those envelopes match the J.M. card delivery tracking numbers provided by bank investigators.

l. According to bank investigators, at approximately 2:42 p.m., all three J.M. debit cards were activated online.

m. At approximately 2:50 p.m., USSS agents conducting physical surveillance at the Avenue I 7-11 saw and

---

[2] According to NFCU investigators, V.H.K. is an earlier victim of this same fraud scheme.

video-recorded AMOS make multiple ATM transactions while the AMOS CAR was parked outside.

n. Agents saw AMOS threw receipts into the trashcan next to the ATM. At approximately 3:30 p.m., I removed the trash and found four ATM receipts for $300 cash withdrawals. The account numbers matched the account numbers for J.M. provided by NFCU investigators.

o. According to NFCU investigators, two of the J.M. debit cards were used to make four $300 withdrawals, thus cashing each card out to its $600 daily cash withdrawal limit, for a total of $1200. NFCU then locked the account and prevented AMOS from withdrawing cash on the third card. NFCU investigators reported that the ATM was then used to make balance inquiries of J.M.'s account.

D. AMOS's Takeover Scheme Targeted Elderly Victims and Resulted in Substantial Loss

p. According to information provided by NFCU investigators, the victims of AMOS's takeover scheme are all over 60 years old.

q. According to information provided by NFCU investigators, to date, AMOS's scheme has resulted in more than $400,000 financial loss.

VI. TRAINING AND EXPERIENCE REGARDING FRAUD SCHEMES

15. Based on my knowledge, training, and experience, as well as information related to me by other law enforcement officers and USSS special agents who specialize in fraud investigations, I know the following:

a. It is common practice for people involved in financial fraud, access device fraud, and identity theft to maintain evidence of their schemes in their homes and cars, and on their digital devices. For example, fraudsters may keep ATM receipts, bank receipts, purchase receipts and other transaction records in hard copy format. They often keep accounting software, spreadsheets, or notes in digital devices to track their transactions. They also often keep track of the names and addresses of co-conspirators either in hard copy format or on digital devices. Additionally, information regarding deposits and withdrawals, along with account numbers, is likely to be found on digital devices or on hard copy printouts.

b. It is common practice for people involved in financial fraud, access device fraud, and identity theft to use and maintain digital devices to store information about their fraud and identity theft crimes long after the crimes have been committed. This information can include logs of fraudulent transaction history, records of funds received, records of payments to or from co-conspirators, communications with co-

conspirators regarding criminal activity, and information regarding victims, including victim profiles and PII.

c. Identity thieves often use digital devices to perpetrate their crimes due to the relative anonymity gained by conducting financial transactions electronically on the Internet. These individuals use digital devices for purposes of, among other things: (i) applying online for fraudulent credit cards; (ii) obtaining PII for the purposes of establishing or modifying fraudulent credit card accounts; (iii) using fraudulently obtained credit cards to make purchases; (iv) manufacturing counterfeit identification, credit cards, and checks; and (v) keeping records of their crimes.

d. Based on my training and experience, I know that individuals who participate in identity theft, bank fraud, and access device fraud schemes often maintain telephone numbers, email addresses, and other contact information and communications involving their co-conspirators in order to conduct their business. Often they do so on their digital devices. Suspects often use their digital devices to communicate with co-conspirators by telephone, e-mail, text messages, and social media.

VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

16. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing

data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in

the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded

onto a hard drive, deleted, or viewed via the Internet.[3] Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive

[3] These statements do not generally apply to data stored in volatile memory such as random-access memory, or "RAM," which data is, generally speaking, deleted once a device is turned off.

requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence

in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by

using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

17. As discussed herein, based on my training and experience I believe that digital devices will be found during the search. I know from my training and experience and my review of publicly available materials that Apple Inc., Motorola, HTC, and Samsung, among other companies, produce devices that can be unlocked by the user with a numerical or an alpha-numerical password, or, for some newer versions of the devices, with a fingerprint placed on a fingerprint sensor. Each company has a different name for its fingerprint sensor feature; for example, Apple's is called "Touch ID." Once a user has set up the fingerprint sensor feature in the security settings of the device, the user can unlock the device by placing a finger or thumb on the device's fingerprint sensor. If that sensor recognizes the fingerprint or thumbprint, the

device unlocks. Most devices can be set up to recognize multiple prints, so that different prints, not necessarily from the same person, will unlock the device. In my training and experience, users of devices with a fingerprint sensor feature often enable that feature, because it unlocks the phone more quickly than the entry of a passcode or password but still offers a layer of security.

18. In some circumstances, fingerprint sensors will not work, and a passcode must be entered to unlock the device. For example, with Apple, Touch ID will not work if (1) more than 48 hours have passed since the device has been unlocked, (2) the device has been turned on or restarted, (3) the device has received a remote lock command, or (4) five attempts to match a fingerprint have been unsuccessful. Other brands have similar restrictions. I do not know the passcodes of the devices likely to be found at the AMOS HOME.

19. For these reasons, while executing the warrant, agents will likely need to use the fingerprints or thumbprints of any user(s) of any fingerprint sensor-enabled device(s) to attempt to gain access to that device while executing the search warrant. The warrant seeks the authority to compel the use of the fingerprint and/or thumbprint of every person who is located at the AMOS HOME during the execution of the search and who is reasonably believed by law enforcement to be a user of a fingerprint sensor-enabled device that is located at the AMOS HOME and falls within the scope of the warrant. The government may not be able to obtain the contents of the devices if those

fingerprints are not used to access the devices by depressing them against the fingerprint sensor at the time of the search. Although I do not know which of the fingers are authorized to access on any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors, and in any event all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

20. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VIII. CONCLUSION

21. For all the reasons described above, there is probable cause to believe that AMOS violated Title 18, United States Code, Section 1029(a)(2) (use of unauthorized access devices).

//

//

//

//

//

//

//

//

//

//

//

//

22. Additionally, there is probable cause to believe that evidence, fruits, and instrumentalities of the offenses described in Attachment B will be found at the premises described in Attachment A.

/s/

ROBERT HAWKEYE NORMAN
Special Agent
United States Secret Service

Subscribed to and sworn before me this 2 day of June 2017.

JACQUELINE CHOOLJIAN

UNITED STATES MAGISTRATE JUDGE